UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
COURT FILE NO.: 17-cv-4196

Margaret Amadick, Jeannie Ball, Jennifer Ball, Thomas Greenwood, Robert Roehl, Constance Zasada, and Theodore Zasada on behalf of themselves and all others similarly situated, Plaintiffs, v. Equifax Information Services, LLC, Defendant.	**CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs (all together "Plaintiffs"), Margaret Amadick, Jeannie Ball, Jennifer Ball, Thomas Greenwood, Robert Roehl, Constance Zasada, and Theodore Zasada on behalf of themselves and all others similarly situated, by and through their attorney, bring this action against Equifax Information Services, LLC (herein after "Defendant"), and hereby allege as follows:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all other similarly situated persons (i.e., the Class Members), whose personally identifiable information, including names, addresses, dates of birth, driver's licenses, Social Security numbers (collectively referred to as "PII") and credit account information (collectively referred to as "CAI"), entrusted to

Defendant was made accessible to a thief or thieves while in the possession, custody and control of Defendant.

2. Through information and belief, from approximately May of 2017, through the present date, documentation containing the PII/CAI of Plaintiffs and thousands of other putative Class Members was left exposed, unprotected, and/or otherwise subject to theft by third parties who otherwise had no reason to be in possession of such information.

3. Defendant disregarded Plaintiffs' and the other Class Members' privacy rights by intentionally, willfully, recklessly and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/CAI from unauthorized disclosure. Plaintiffs' and Class Members' PII/CAI was compromised and/or stolen.

4. Defendant's intentional, willful, reckless and/or negligent disregard of Plaintiffs' and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiffs' and Class Members' PII/CAI. The improper use of PII/CAI by unauthorized third parties can result in an adverse impact on, among other things, a victim's credit rating and finances. The type of wrongful PII/CAI disclosure made by Defendant is the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of that PII/CAI.

5. On behalf of themselves and Class Members, Plaintiffs have standing to bring this lawsuit because they were damaged as a direct and/or proximate result of

Defendant's wrongful actions and/or inaction and the resulting Data Breach.

6. Defendant's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identify theft and identify fraud.[1] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identify Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/CAI is subject to a reported data breach, such as the Data Breach at issue here, are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft.

7. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiffs' and Class Members' PII/CAI have not yet used the information but will do so later, or re-sell it. Even without such loss, Plaintiffs and Class Members are entitled to relief and recovery, including statutory damages under federal privacy statutory provisions as set forth herein.

8. Defendant's failure to safeguard and secure Plaintiffs' and Class Members' PII/CAI violated the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721, et seq.

9. Defendant's failure to safeguard and secure Plaintiffs' and Class Members' PII/CAI

[1] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/CAI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud, and government fraud (theft of government services).

violated the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 et seq.

10. Therefore, Defendant failed to adopt, implement, and/or maintain adequate procedures to protect such information and limit its dissemination to the permissible purposes under the FCRA. In further violation of the FCRA, Defendant failed to protect and wrongfully disseminated Plaintiffs' and Class Members' PII/CAI, which is personal identifying information, specifically defined in, and protected by, the FCRA. As a direct and proximate result of Defendant's willful, reckless and/or grossly negligent violations of the FCRA, an unauthorized third party (or parties) obtained Plaintiffs' and Class Members' PII/CAI for no permissible purpose under FCRA.

11. Defendant's wrongful actions and/or inaction also constitute common law negligence and common law invasion of privacy by public disclosure of private facts.

12. Plaintiffs, on behalf of themselves and the Class Members, seek actual damages, economic damages, statutory damages, nominal damages, exemplary damages, injunctive relief, attorney's fees, litigation expenses and costs of suit.

I. JURISDICTION

13. Jurisdiction of this court arises under 18 U.S.C. § 2721, 28 U.S.C. § 1331 (Federal Question), 28 U.S.C. § 1337 (Commerce), 15 U.S.C. § 1681 et seq., 18 U.S.C. § 2724(a) (DPPA) and 28 U.S.C. § 1367 (Supplemental).

14. Venue is appropriate in this Court pursuant to 28 U.S.C. § 1391.

15. This Court has personal jurisdiction over Defendant because, at all relevant times,

Defendant conducted, and continues to conduct, substantial business in the District of Minnesota.

16. Venue is proper in the District of Minnesota pursuant to 28 U.S.C. §1391(b); a substantial part of the events giving rise to this action occurred in the District of Minnesota and Defendant conducts substantial business in the District of Minnesota.

II. PARTIES

17. Plaintiff Margaret Amadick is an individual consumer currently residing in the City of White Bear Lake, Ramsey County, State of Minnesota. Plaintiff Amadick was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

18. Plaintiff Jeannie Ball is an individual consumer currently residing in the City of Duluth, St. Louis County, State of Minnesota. Plaintiff Jeannie Ball was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

19. Plaintiff Jennifer Ball is an individual consumer currently residing in the City of Duluth, St. Louis County, State of Minnesota. Plaintiff Jennifer Ball was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

20. Thomas Greenwood is an individual consumer currently residing in the City of Forest City, Winnebago County, State of Iowa. Plaintiff Thomas Greenwood was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

21. Plaintiff Robert Roehl is an individual consumer currently residing in the City of Hinckley, Pine County, State of Minnesota. Plaintiff Robert Roehl was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

22. Plaintiff Constance Zasada is an individual consumer currently residing in the Village of Clayton, Polk County, State of Wisconsin. Plaintiff Constance Zasada was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

23. Plaintiff Theodore Zasada is an individual consumer currently residing in the Village of Clayton, Polk County, State of Wisconsin. Plaintiff Theodore Zasada was and is a "person" as defined under 18 U.S.C. § 2725(2), is a "consumer" as that term is defined by 15 U.S.C. § 1681a(c), and is protected by and entitled to enforce the remedies of the DPPA and FCRA.

24. According to Defendant's own records Plaintiffs' PII/CAI was subjected to the aforementioned Data Breach.

25. Plaintiffs' PII/CAI, which was entrusted to Defendant and which Defendant failed to properly safeguard, was stolen from Defendant on or about May of 2017, through the present.

26. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs have suffered actual harm. Defendant's wrongful disclosure of and failure to safeguard Plaintiffs' PII/CAI has also placed Plaintiffs at an imminent, immediate, and continuing increased risk of harm for identity theft and identity fraud as recognized by Defendant in its press releases and website information.

27. Defendant, Equifax Information Services, LLC is organized under the laws of Georgia, has a principal place of business at 1550 Peachtree Street, NW, Atlanta, Georgia 30309, and is authorized to do business in Minnesota.

28. Defendant was and is a "person" as defined under 18 U.S.C. § 2725(2) and 15 U.S.C. § 1681a(b), is a "consumer credit reporting agency," as defined by 15 U.S.C. § 1681a(f) of the Act, regularly engaged in the business of assembling, evaluating, and dispersing information concerning consumers for the purpose of furnishing "consumer reports," as defined in § 1681a(d) of the Act, to third parties, and is restricted by, and subject to, the remedies of the DPPA and FCRA.

III. FACTUAL ALLEGATIONS

29. In the regular course of its business, Defendant collects and maintains possession, custody, and control of a wide variety of Plaintiffs' and Class Members' personal

and confidential information, including: names, addresses, dates of birth, Social Security numbers, drivers' license information, credit information, and banking information (collectively referred to as "PII/CAI").

30. In May of 2017, through the present, and, at this time unknown, third party or third parties exploited a U.S. website application vulnerability to gain access to certain files in Defendant's possession, custody, and control.

31. Between May of 2017, through the present, an untold number of files containing Plaintiffs' and Class Members' PII/CAI were viewed and/or used by some unknown third party or third parties.

32. Defendant waited until September 7, 2017, to disclose that from May to July 2017, the PII/CAI of millions of individuals including Plaintiffs and the putative class described herein had been accessed by an unauthorized third party or third parties.

33. Given the substantial delay of Defendant's disclosure of the Data Breach, the Plaintiffs' and Class Members' PII/CAI could have been bought and sold several times on the robust international cyber black market while the Plaintiffs and Class Members would have had no chance whatsoever to take measures to protect their privacy.

34. Defendant's wrongful actions and/or inaction—failing to protect Plaintiffs' and Class Members' PII/CAI with which it was entrusted—directly and/or proximately caused the theft and dissemination of Plaintiffs' and Class Members' PII/CAI without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Defendant's wrongful actions and/or inaction,

Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/CAI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under the DPPA for which they are entitled to compensation.

35. As a result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/CAI, Plaintiffs' and Class Members' privacy has been invaded and their rights violated. Their compromised PII/CAI was private and sensitive in nature and was left inadequately protected by Defendant. Defendant's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

36. Identity theft occurs when a person's PII/CAI, such as the person's name, e-mail address, address, Social Security number, billing and shipping addresses, phone number and credit card information are used without his or her permission to

commit fraud or other crimes.[2]

37. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[3] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII/CAI]."[4] The FTC estimates that the identities of as many as 9 million Americans are stolen each year. Id.

38. As a direct and/or proximate result of the Data Breach, Plaintiffs and Class Members will now be required to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

39. Because Plaintiffs' and Class Members' Social Security numbers were stolen

---

[2] See http://www.consumer.ftc.gov/features/feature-0014-identiy-theft.

[3] Protecting Consumer Privacy in an Era of Rapid Change FTC Report (March 2012) (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[4] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, 35-38 (Dec. 2010), available at http:www.ftc.gov/os/2010/12/101201privacyreport.pdf; Comment of Center for Democracy & Technology, cmt. #00469, at 3; Comment of Staz, Inc., cmt. #00377, at 11-12.

and/or compromised, they also now face a significantly heightened risk of identity theft.

40. According to the FTC, identity theft is serious. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[5]

41. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/CAI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's access to credit, credit rating, and finances. Moreover, unlike other PII/CAI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

42. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs

[5] *See* Federal Trade commission, *Signs of Identity Theft,* http://www.consumer.ftc.gov/articles/0271-signs-identity-theft.

using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

43. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.6 Thus, a person whose PII/CAI has been stolen cannot obtain a new Social Security number until the damage has already been done.

44. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more

[6] *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html).

difficult to obtain credit due to the absence of a credit history.

45. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the Data Breach, the thieves and/or their customers now have Plaintiffs' and Class Members' PII/CAI. As such, Plaintiffs and Class Members have been deprived of the value of their PII/CAI.[7]

46. Plaintiffs' and Class Members' PII/CAI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years. Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[8]

---

[7] See, e.g., John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII/CAI") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009)("PII/CAI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.")(citations omitted); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#. UGRgtq7yBR4.

[8] StopTheHacker, The "Underground Credit Card Blackmarket, http://stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket.

47. The Data Breach was a direct and/or proximate result of Defendant's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiffs' and Class Members' PII/CAI from unauthorized access, use, and/or disclosure, as required by various state regulations and industry practices.

48. Defendant flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/CAI to protect against anticipated threats to the security or integrity of such information. Defendant's security deficiencies allowed unauthorized individuals to access, remove from its premises, transport, disclose, and/or compromise the PII/CAI of thousands of individuals, including Plaintiffs and Class Members.

49. Defendant's wrongful actions and/or inaction directly and proximately caused the theft and dissemination of Plaintiffs' and Class Members' PII/CAI without their knowledge, authorization, and consent. As a direct and proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred damages in the form of, inter alia: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/CAI; (iii) loss of privacy; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon

them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under the DPPA and the FCRA, for which they are entitled to compensation.

IV. CLASS ALLEGATIONS

50. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this class action as a national class action on behalf of themselves and the following Class of similarly situated individuals:

51. All persons residing in the states of Minnesota, Iowa, and Wisconsin whose personal identifying information (PII/CAI) was stolen and/or exposed to potential theft from Defendant Equifax by unknown third parties between May of 2017, through the present.

52. Excluded from the Class are the (i) owners, officers, directors, employees, agents and/or representatives of Defendant Equifax and their parent entities, subsidiaries, affiliates, successors, and/or assigns, and (iii) the Court, Court personnel, and members of their immediate families.

53. The putative Class is, through information and belief, comprised of thousands of persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

54. The rights of each Class Member were violated in a virtually identical manner as

a result of Defendant's willful, reckless, and/or negligent actions and/or inactions.

55. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, inter alia:

(a) Whether Defendant violated the DPPA and the FCRA by failing to properly secure Plaintiffs' and Class Members' PII/CAI;

(b) Whether Defendant willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/CAI;

(c) Whether Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/CAI;

(d) Whether Defendant breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/CAI;

(e) Whether Defendant was negligent in failing to secure Plaintiffs' and Class Members' PII/CAI;

(f) Whether by disclosing or exposing Plaintiffs' and Class Members' PII/CAI without authorization, Defendant invaded Plaintiffs' and Class Members' privacy; and

(g) Whether Plaintiffs and Class Members sustained damages as a result of Defendant's failure to secure and protect their PII/CAI.

56. Plaintiffs' claims are typical of the claims of the Class, which all arise from the same operative facts and are based on the same legal theories, including:

(a) The recovery of statutory and punitive damages for Defendant's violations of

federal and state privacy laws.

57. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs are committed to vigorously litigating this matter. Further, Plaintiffs have secured counsel experienced in handling consumer rights class actions. Neither Plaintiffs nor their counsel has any interests that might cause them not to vigorously pursue this case.

58. This action should be maintained as a Class action because the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members which would establish incompatible standards of conduct for the parties opposing the Class.

59. A Class action is a superior method for the fair and efficient adjudication of controversy. The interest of Class members in individually controlling prosecution of separate claims against Defendant is small. Management of the Class claims is likely to present significantly fewer difficulties than those presented in many individual claims. The identities of the Class members may be obtained using Defendant's records.

60. Class certification, therefore, is appropriate pursuant to FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

61. Class certification also is appropriate pursuant to FED. R. CIV. P. 23(b)(2)

because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the class as a whole.

62. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

V. CAUSES OF ACTION

COUNT I.

DRIVER'S PRIVACY PROTECTION ACT

63. Plaintiffs incorporate by reference all the foregoing paragraphs.

64. Defendant willfully and/or negligently violated provisions of the Driver's Privacy Protection Act. Defendant's violations include, but are not limited to the following:

(a) Defendant violated 18 U.S.C. §§ 2721 et. seq. by willfully and/or negligently failing to specifically protect and limit the dissemination of Plaintiffs' and Class Members' PII/CAI into the public domain, as was and is contrary to established State and Federal law.

65. As a result of the above and continuing violations of the DPPA, Defendant is liable to the Plaintiffs in the sum of Plaintiffs' actual damages, statutory damages, punitive damages, costs, disbursements, and reasonable attorneys' fees, along with any appropriate injunctive relief.

COUNT II.

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

66. Plaintiffs incorporate by reference all the foregoing paragraphs.

67. Defendant's failure to secure and protect Plaintiffs' and Class Members' PII/CAI directly resulted in the public disclosure of such private information.

68. Dissemination of Plaintiffs' and Class Members' PII/CAI is not of a legitimate public concern; publicity of their PII/CAI would be, is, and will continue to be offensive to reasonable people.

69. Plaintiffs and the Class Members were, and continue to be, damaged as a direct and/or proximate result of invasion of their privacy by publicly disclosing their private facts (i.e., their PII/CAI) in the form of, inter alia: (i) improper disclosure of their PII/CAI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress, for which they are entitled to compensation. At the very least, Plaintiffs and the Class Members are entitled to nominal statutory damages.

70. Defendant’s wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an ongoing invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (i.e., their PII/CAI).

COUNT III.

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

71. Plaintiffs incorporate by reference all the foregoing paragraphs.

72. The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies, of which Defendant is, to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

73. As a Consumer Reporting Agency, Defendant is required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiffs' and Class Members' PII/CAI) in a manner fair and equitable to consumers while maintaining the "confidentiality, accuracy, relevancy and proper utilization of such information. Defendant, however, violated the FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of Plaintiffs' and Class Members' PII/CAI and its wrongful dissemination. By way of example, Defendant could have:

a. Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures.

b. Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews and ensure that these metrics were an integral part of Defendant’s corporate governance program.

74. On information and belief, Defendant took none of these proactive actions to secure and protect Plaintiffs' and Class Members' PII/CAI.

75. Plaintiffs' and Class Members' PII/CAI, in whole or in part, constitutes personal identifying information as defined by the FCRA. Defendant violated the FCRA by failing to specifically protect and limit the dissemination of Plaintiffs' and Class Members' PII/CAI.

76. As a direct and/or proximate result of Defendant's willful and/or reckless violations of FCRA, as described above, Plaintiffs' and Class Members' PII/CAI was stolen and/or made accessible to unauthorized third parties.

77. As a direct and/or proximate result of Defendant willful and/or reckless violations of FCRA, as described above, Plaintiffs and Class Members were, and continue to be, damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

78. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as

attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §168ln(a).

COUNT IV.

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

79. Plaintiffs incorporate by reference all the foregoing paragraphs.

80. In the alternative, and as described above, Defendant negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiffs' and Class Members' PII/CAI for the permissible purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft and dissemination of Plaintiffs' and Class Members' PII/CAI. By way of example, Defendant could have:

a. Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures.

b. Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, and ensure that these metrics were an integral part of Defendant’s corporate governance program.

81. On information and belief, Defendant took none of these proactive actions to secure and protect Plaintiffs' and Class Members' PII/CAI.

82. It was reasonably foreseeable that Defendant’s failure to implement and maintain procedures to protect and secure Plaintiffs' and Class Members' PII/CAI would result in an unauthorized third party gaining access to their PII/CAI for no

permissible purpose under FCRA.

83. As a direct and/or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs' and Class Members' PII/CAI was stolen and/or made accessible to unauthorized third parties in the public domain.

84. As a direct and/or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs and the Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of- pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

85. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages, including, inter alia: (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT V.

NEGLIGENCE

86. Plaintiffs incorporate by reference all the foregoing paragraphs.

87. Defendant had a duty to exercise reasonable care in safeguarding and protecting

Plaintiffs' and Class Members' PII/CAI.

88. Defendant violated its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/CAI, as set forth in detail above.

89. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/CAI would result in an unauthorized third party gaining access to such information for no lawful purpose.

90. Plaintiffs and the Class Members were, and continue to be, damaged as a direct and/or proximate result of Defendant's failure to secure and protect their PII/CAI in the form of, inter alia, (i) improper disclosure of their PII/CAI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress- for which they are entitled to compensation.

91. Defendant's wrongful actions and/or inaction (as described above) constituted negligence at common law.

COUNT VI.

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

92. Plaintiffs incorporate by reference all the foregoing paragraphs.

93. Defendant's failure to secure and protect Plaintiffs' and Class Members' PII/CAI directly resulted in the public disclosure of such private information.

94. Dissemination of Plaintiffs' and Class Members' PII/CAI is not of a legitimate public concern; publicity of their PII/CAI would be, is, and will continue to be, offensive to a reasonable person.

95. Plaintiffs and the Class Members were, and continue to be, damaged as a direct and/or proximate result of Defendant's actions in the form of, inter alia: (i) improper disclosure of their PII/CAI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress- for which they are entitled to compensation. At the very least, Plaintiffs and the Class Members are entitled to nominal damages.

96. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, an ongoing invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (i.e., their PII/CAI).

VI. REQUEST FOR RELIEF

97. DAMAGES. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction (as described above), Plaintiffs and Class Members suffered (and continue to suffer) damages in the form of, inter alia: (i) the untimely and/or

inadequate notification of the Data Breach; (ii) improper disclosure of their PII/CAI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/CAI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under the DPPA and the FCRA, for which they are entitled to compensation. Plaintiffs and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiffs' and Class Members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court.

98. EXEMPLARY DAMAGES. Plaintiffs and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

99. INJUNCTIVE RELIEF. Plaintiffs and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring Defendant to, inter alia, (i) immediately disclose to Plaintiffs and Class Members the precise nature and extent of their PII/CAI contained within the files stolen by and/or otherwise accessed by the third party or third parties who engaged in the Date Breach, (ii) make a prompt and detailed disclosure to all individuals affected by any actual or potential data breaches of their PII/CAI, (iii) immediately secure the PII/CAI of all individuals affected by any actual or potential data breaches of their PII/CAI, (iv) implement the above- referenced proactive policies and procedures in order to secure and

protect individuals' PII/CAI and be in a position to immediately notify them about any data breaches, (v) submit to periodic compliance audits by a third party regarding the implementation of, and compliance with, such policies and procedures, and (vi) submit to periodic compliance audits by a third party regarding the security of individuals' PII/CAI within its possession, custody and control.

100. ATTORNEY'S FEES, LITIGATION EXPENSES AND COSTS. Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, inter alia, 18 U.S.C. § 2724 (b)(3) and 15 U.S.C. §§ 1681n(a); o(a).

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request that (i) Defendant be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon a jury trial, judgment be awarded against Defendant, in favor of Plaintiffs and the Class Members, for:

- actual damages, consequential damages, DPPA and FCRA statutory damages and/or nominal damages (as described above) in an amount to be determined by the trier of fact;
- punitive damages;
- exemplary damages:

- injunctive relief as set forth above;
- pre- and post-judgment interest at the highest applicable legal rates;
- attorney's fees and litigation expenses incurred through trial;
- costs of suit; and
- such other and further relief that this Court deems just and proper.

VII. JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

Dated this 8th day of September, 2017.

Respectfully submitted,

By: s/Thomas J. Lyons Jr.
Thomas J. Lyons Jr., Esq.
Attorney I.D. #: 0249646
CONSUMER JUSTICE CENTER P.A.
367 Commerce Court
Vadnais Heights, MN 55127
Telephone: 651-770-9707
Facsimile: 651-704-0907
tommy@consumerjusticecenter.com

Thomas J. Lyons, Esq.
Attorney I.D. #: 65699
LYONS LAW FIRM P.A.
367 Commerce Court
Vadnais Heights, MN 55127
Telephone: 651-770-9707
Facsimile: 651-770-5830
Email: tlyons@lyonslawfirm.com

ATTORNEYS FOR PLAINTIFFS